

BÁO CÁO THỰC HÀNH

Môn học: **Hệ thống tìm kiếm, phát hiện và ngăn ngừa xâm nhập**

Lab 02 – Triển khai Snort Inline

GVHD: Đỗ Hoàng Hiến

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT204.O21.ANTT.2

STT	Họ và tên	MSSV	Email
1	Nguyễn Viết Dũng	21520747	21520090@gm.uit.edu.vn
2	Lưu Thị Huỳnh Như	21521242	21521112@gm.uit.edu.vn
3	Lê Đoàn Trà My	21521149	21521149@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Công việc	Kết quả tự đánh giá
1	Yêu cầu 1	100%
2	Yêu cầu 2	100%
3	Yêu cầu 3	100%

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

¹ Ghi nội dung công việc, yêu cầu trong bài Thực hành

BÁO CÁO CHI TIẾT

1. Yêu cầu 1: Sinh viên trả lời các câu hỏi bên dưới

1.1a. Tìm hiểu về Snort? Snort cho phép chạy trên những chế độ (mode) nào?

→ Snort là một NIDPS mã nguồn mở dựa trên kỹ thuật phát hiện Signature-based NIDPS. Sử dụng một tập các bộ rules định nghĩa dấu hiệu của tấn công cho việc nhận diện tấn công. Quản trị viên mạng có thể phát hiện các cuộc tấn công từ chối dịch vụ DoS, tấn công DoS phân tán DDoS, tấn công CGI (Common Gateway Interface), tràn bộ đệm, scan port,...

* Snort cho phép chạy trên các mode:

- Sniff mode (snort -v): thu thập và phân tích gói tin.
- Packet logger mode (snort -l /var/log/snort): tập hợp packet nó thấy và đưa vào log
- NIDS mode (snort -c /etc/snort/snort.conf -I eth0): Chế độ chính của Snort, phát hiện tấn công/hành vi xâm nhập độc hại.
- Inline mode: cho phép phân tích các gói tin từ firewall iptables sử dụng các tập lệnh mới như: pass, drop, reject để ngăn chặn các hoạt động độc hại.

1.1b. Trình bày những tính năng chính của Snort?

→ Tính năng chính của Snort:

- Bắt lưu lượng mạng đang truyền và phân tích lưu lượng mạng theo thời gian thực.
- Phân tích giao thức, tìm kiếm/so khớp nội dung.
- Ghi log các sự kiện, thông tin.
- Nhận diện, phát hiện tấn công hoặc do thám dựa trên các rules và các thông tin phân tích được.

2. Yêu cầu 2: Cài đặt và cấu hình Snort Inline theo các bước bên dưới. Chụp lại các hình ảnh minh chứng (chụp full màn hình) cho từng bước làm

Mô hình mạng triển khai sẽ là: **10.81.27.0/24** và **192.168.27.0/24**, trong đó 2 là chữ số cuối trong MSSV của Huỳnh Như, và 7 là chữ số cuối trong MSSV của Việt Dũng.

2.1a. Cấu hình mạng cho các máy theo mô hình

- Kiểm tra card VMnet8 (NAT) đã tồn tại và được bật DHCP:

- Gán các card mạng cho máy Router:

- Gán các card mạng cho máy Kali:

- Gán các card mạng cho máy Snort:

- Gán các card mạng cho máy Victim:

2.1b. Cấu hình địa chỉ IP cho các máy

Kali Linux - VM Player

File Edit View VM Tabs Help

Normal x1 kb-linux-2023.3-memoria-grandis x2 KALI Linux 1 x3 VM A x4 VM B x5 MatejGlab202-Linux x6 openmint x7

1 2 3 4 5 6 7

File Actions Edit View Help

kali@kali:~\$ ifconfig

```

eth0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether 02:02:00:00:00:02 txqueuelen 0 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 (frame 0)
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether 00:0c:29:c7:c4:c9 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth2: flags=4161<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.81.27.100 netmask 255.255.255.0 broadcast 10.81.27.255
    ether f0:0b:3b:13:9f:fe:c7:c4:c9 txqueuelen 0 (Ethernet)
    RX packets 100 bytes 1124 (7.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    RX packets 100 bytes 1124 (7.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 1<lo>
    txqueuelen 1000 (Local Loopback)
    RX packets 126 bytes 1124 (7.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 126 bytes 1124 (7.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

kali@kali:~\$

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

* Cấu hình địa chỉ IP máy Victim:

- Nhập lệnh **sudo nano /etc/network/interfaces** và thay đổi nội dung để chỉnh IP:

```

GNU nano 2.0.7 File: /etc/network/interfaces Modified
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).
# The loopback network interface
auto lo;
iface lo inet loopback
# The primary network interface
auto eth0;
iface eth0 inet static
address 192.168.27.200
netmask 255.255.255.0
gateway 192.168.27.1
    
```

- Restart network: **sudo /etc/init.d/networking restart**

- Kiểm tra IP máy Victim sau khi config

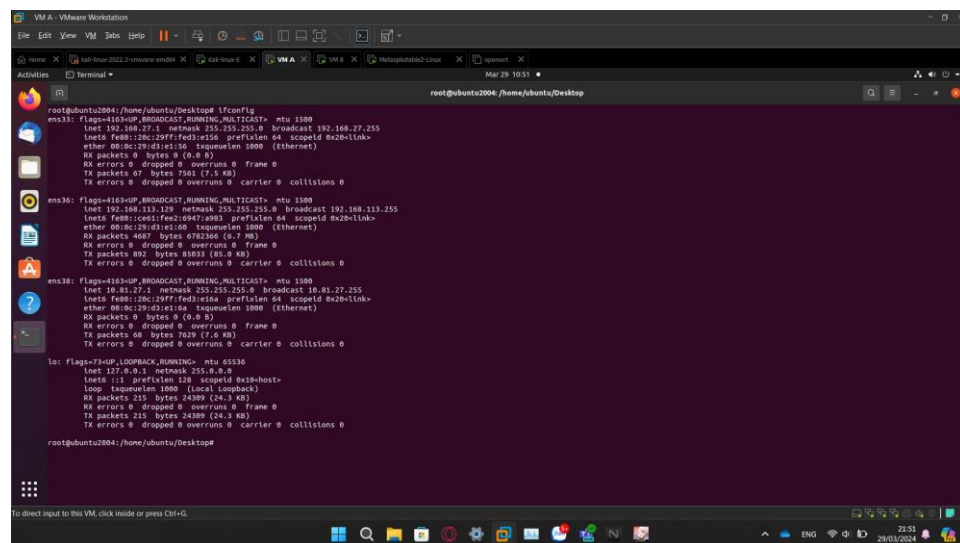
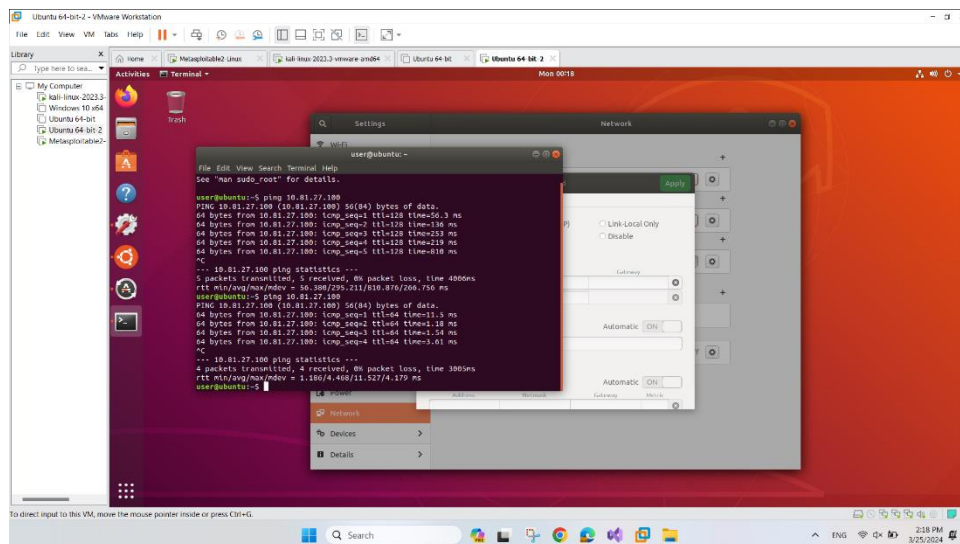
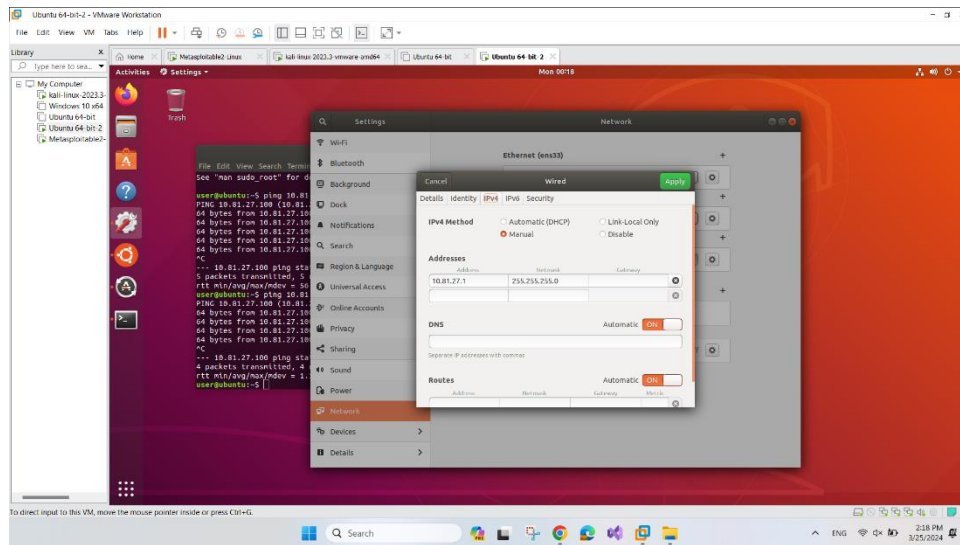
```

RX bytes:40393 (39.4 KB) TX bytes:40393 (39.4 KB)
mifadim@metasploitable:~$ sudo /etc/init.d/networking restart
* Restarting networking: networking:~
mifadim@metasploitable:~$ ifconfig
eth0
Link encap:Ethernet  Hardware: 08:00:27:1b:1b:2b
inet addr:192.168.27.200 Bcast:192.168.27.255 Mask:255.255.255.0
netmask: 255.255.255.0 broadcast: 192.168.27.255
UP BROADCAST RUNNING MULTICAST  MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0;
RX bytes:0 (0.0 KB) TX bytes:0 (0.0 KB)
Interrupt:17 Base address:0x0000

lo
Link encap:(inet) Loopback
inet addr:127.0.0.1 Bcast:127.0.0.1
netmask: 255.255.255.255 MTU:65536 Metric:1
UP LOOPBACK RUNNING  MTU:65536 Metric:1
RX packets:154 errors:0 dropped:0 overruns:0 frame:0
TX packets:154 errors:0 dropped:0 overruns:0 carrier:0
collisions:0;
RX bytes:42613 (41.6 KB) TX bytes:42613 (41.6 KB)

mifadim@metasploitable:~$ _
    
```

* Cài đặt IP cho máy Router



* Máy Snort:

```

root@ubuntu2004:/etc/snort# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.10 netmask 255.255.255.0 broadcast 192.168.1.255
    ether 08:00:27:0d:6e:5a txqueuelen 1000 (Ethernet)
    RX packets 196 bytes 30349 (30.3 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 285 bytes 41410 (41.4 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ens36: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.130 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::143c:650f:532b:3771 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:0d:6e:04 txqueuelen 1000 (Ethernet)
    RX packets 929 bytes 122582 (122.5 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 481 bytes 52036 (52.0 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ens38: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet6 fe80::143c:650f:532b:3771 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:0d:6e:0e txqueuelen 1000 (Ethernet)
    RX packets 123 bytes 15069 (15.0 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 193 bytes 22973 (22.9 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (local loopback)
    RX packets 0 bytes 0 (0.0 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@ubuntu2004:/etc/snort#

```

2.1c. Cấu hình NAT outbound cho máy router

- Cấu hình NAT outbound cho máy router bằng cách sử dụng công cụ iptables:

```

root@ubuntu2004:/# sudo apt-get install iptables

```

- Cấu hình bảng NAT của router bằng các câu lệnh:

```
iptables -t nat -A POSTROUTING -o ens36 -j MASQUERADE
```

```
iptables -A FORWARD -I ens38 -o ens36 state -m --state RELATED,ESTABLISHED -j ACCEPT
```

```
iptables -A FORWARD -I ens33 -o ens36 state -m --state RELATED,ESTABLISHED -j ACCEPT
```

- Cuối cùng là lưu lại cấu hình bằng câu lệnh:

```
sh -c "iptables-save > /etc/iptables/rules.v4"
```

* Kết quả cấu hình bằng iptables và bảng NAT:

```

root@ubuntu2004:/# iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source                destination

Chain INPUT (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source                destination
MASQUERADE all  --  anywhere              anywhere
root@ubuntu2004:/# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination
ACCEPT     all  --  anywhere              anywhere    state RELATED,ESTABLISHED
ACCEPT     all  --  anywhere              anywhere    state RELATED,ESTABLISHED

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
root@ubuntu2004:/#

```

- Máy attacker ping google.com:

```

(kali㉿kali)-[~/Desktop]
$ ping -w 4 google.com
PING google.com (142.251.220.78) 56(84) bytes of data:
64 bytes from hkg07s51-in-f14.1e100.net (142.251.220.78): icmp_seq=1 ttl=127 time=37.2 ms
64 bytes from hkg07s51-in-f14.1e100.net (142.251.220.78): icmp_seq=2 ttl=127 time=49.9 ms
64 bytes from hkg07s51-in-f14.1e100.net (142.251.220.78): icmp_seq=3 ttl=127 time=37.7 ms
64 bytes from hkg07s51-in-f14.1e100.net (142.251.220.78): icmp_seq=4 ttl=127 time=33.7 ms

— google.com ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 33.656/39.615/49.946/6.162 ms

(kali㉿kali)-[~/Desktop]
$

```

- Traceroute ở máy attacker:


```
(kali@kali)-[~/Desktop]
$ traceroute google.com
traceroute to google.com (142.251.220.46), 30 hops max, 60 byte packets
 1  10.81.27.1 (10.81.27.1)  2.248 ms  1.392 ms  0.940 ms
 2  192.168.30.2 (192.168.30.2)  1.375 ms  1.163 ms  1.081 ms
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

2.1d. Cài đặt và cấu hình Snort

- Cài đặt snort:

```
root@ubuntu2004:/etc/snort# snort -V

    ,,-
   o" )~
    '

-*> Snort! <*-
Version 2.9.7.0 GRE (Build 149)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.9.1 (with TPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11

root@ubuntu2004:/etc/snort#
```

- Tạo file rules riêng cho snort:

```
root@ubuntu2004:/etc/snort# ls rules/
nhom9-snort.rules
root@ubuntu2004:/etc/snort#
```


- Tạo và viết file config cho snort:

```

root@ubuntu2004:/etc/snort# sudo apt-get install snort
E: dpkg was interrupted, you must manually run 'sudo dpkg --configure -a' to correct the problem.
root@ubuntu2004:/etc/snort# apt-get install snort
E: dpkg was interrupted, you must manually run 'sudo dpkg --configure -a' to correct the problem.
root@ubuntu2004:/etc/snort# snort -v
--* Snort! <*-
o" )- Version 2.9.7.0 GRE (Build 149)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.9.1 (with TPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11

root@ubuntu2004:/etc/snort# ls rules/
nhom9-snort.rules
root@ubuntu2004:/etc/snort# cat nhom9-snort.conf
config daq: afpacket
config daq_mode: inline

include /etc/snort/rules/nhom9-snort.rules
root@ubuntu2004:/etc/snort#
  
```

- Kiểm tra:

```

root@ubuntu2004:/etc/snort# snort -t
-----[detection-filter-config]-----
| memory-cap : 1048576 bytes
| none
| none
-----[rate-filter-config]-----
| memory-cap : 1048576 bytes
| none
| none
-----[event-filter-config]-----
| memory-cap : 1048576 bytes
| none
| none
| none
| none
Rule application order: activation->dynamic->pass->drop->sdrop->reject->alert->log
Verifying Preprocessor Configurations!
afpacket daq configured to inline.
Acquiring network traffic from "ens33:ens38".
Decoding Ethernet

=== Initialization Complete ===

--* Snort! <*-
o" )- Version 2.9.7.0 GRE (Build 149)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.9.1 (with TPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11

Snort successfully validated the configuration!
Snort exiting
root@ubuntu2004:/etc/snort#
  
```

- Chạy snort:

```

root@ubuntu2004:/etc/snort

| s+d 0 0 0 0
-----
[detection-filter-config]-----
| memory-cap : 1048576 bytes
-----
[rate-filter-config]-----
| memory-cap : 1048576 bytes
-----
[event-filter-config]-----
| memory-cap : 1048576 bytes
-----
[rule application order: activation->dynamic->pass->drop->sdrop->reject->alert->log]
Verifying Preprocessor Configurations!
afpacket 0M0 configured to inline.
Acquiring network traffic from "ens33:ens33".
Reload thread starting...
Reload thread started, thread 0x7f203634d700 (3479)

=== Initialization Complete ===

-> Snort! <*-
Version 2.9.7.0 GRE (Build 149)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.9.1 (with TPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11

Commencing packet processing (pid=3474)
Decoding Ethernet
  
```

- Máy victim ping google.com:

```

msfadmin@metasploitable:~$ ping -w 4 google.com
PING google.com (142.250.66.78) 56(84) bytes of data.
64 bytes from hkg12s27-in-f14.1e100.net (142.250.66.78): icmp_seq=1 ttl=127 time
=35.1 ms
64 bytes from hkg12s27-in-f14.1e100.net (142.250.66.78): icmp_seq=2 ttl=127 time
=149 ms
64 bytes from hkg12s27-in-f14.1e100.net (142.250.66.78): icmp_seq=3 ttl=127 time
=45.0 ms
64 bytes from hkg12s27-in-f14.1e100.net (142.250.66.78): icmp_seq=4 ttl=127 time
=41.2 ms

--- google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2998ms
rtt min/avg/max/mdev = 35.137/67.828/149.953/47.545 ms
msfadmin@metasploitable:~$
  
```

- Máy attacker ping tới máy victim:

```

(kali@kali)-[~/Desktop]
$ ping -w 4 192.168.27.200
PING 192.168.27.200 (192.168.27.200) 56(84) bytes of data.
64 bytes from 192.168.27.200: icmp_seq=1 ttl=63 time=2.39 ms
64 bytes from 192.168.27.200: icmp_seq=2 ttl=63 time=7.24 ms
64 bytes from 192.168.27.200: icmp_seq=3 ttl=63 time=2.12 ms
64 bytes from 192.168.27.200: icmp_seq=4 ttl=63 time=28.7 ms

— 192.168.27.200 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 2.116/10.107/28.690/10.920 ms
  
```

2.1e. Viết rule cho Snort

- Viết Rules:

alert icmp any any -> 192.168.27.0/24 any (msg: "ICMP detected!!!"; GID:1; sid:10000001; rev:001;)

```

root@ubuntu2004: /etc/snort
alert icmp any any -> 192.168.27.0/24 any (msg: "ICMP detected!!!"; GID:1; SID:10000001; rev:001;)

"rules/nhom9-snort.rules" 2 lines, 100 characters
  
```

- Kiểm tra:

```

root@ubuntu2004: /etc/snort

-----[detection-filter-config]-----
| memory-cap : 1048576 bytes
| none
-----[detection-filter-rules]-----
| none

-----[rate-filter-config]-----
| memory-cap : 1048576 bytes
| none
-----[rate-filter-rules]-----
| none

-----[event-filter-config]-----
| memory-cap : 1048576 bytes
| none
-----[event-filter-global]-----
| none
-----[event-filter-local]-----
| none
-----[suppression]-----
| none

Rule application order: activation->dynamic->pass->drop->sdrops->reject->alert->log
Verifying Preprocessor Configurations!

[ Port Based Pattern Matching Memory ]
afpacket DAG configured to inline.
Acquiring network traffic from "ens33:ens38".
Decoding Ethernet

--- Initialization Complete ---

o*~ Snort! ~*
...- Version 2.9.7.0 GRE (Build 149)
    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
    Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
    Copyright (C) 1998-2013 Sourcefire, Inc., et al.
    Using libpcap version 1.9.1 (with TPACKET_V3)
    Using PCRE version: 8.39 2016-06-14
    Using ZLIB version: 1.2.11

Snort successfully validated the configuration!
Snort exiting
root@ubuntu2004: /etc/snort#
  
```

- Chạy snort và kiểm tra ping từ máy router đến victim:

```

root@ubuntu2004:/etc/snort
Snort successfully validated the configuration!
Snort exiting
root@ubuntu2004:/etc/snort# snort -c nhom9-snort.conf -i ens33:ens38
Enabling inline operation
Running in IDS mode

=== Initializing Snort ===
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "nhom9-snort.conf"
Tagged Packet Limit: 256
Log directory = /var/log/snort

-----
Initializing rule chains...
1 Snort rules read
  1 detection rules
  0 decoder rules
  0 preprocessor rules
  1 Option Chains linked into 1 Chain Headers
  0 Dynamic rules
-----

-----[Rule Port Counts]-----
| src      | tcp | udp | icmp | ip |
| dst      | 0   | 0   | 0    | 0  |
| any      | 0   | 0   | 1    | 0  |
| ac       | 0   | 0   | 1    | 0  |
| sad      | 0   | 0   | 0    | 0  |
-----

-----[detection-filter-config]-----
| memory-cap : 1048576 bytes
| none
-----[detection-filter-rules]-----
| none
-----

-----[rate-filter-config]-----
| memory-cap : 1048576 bytes
| none
-----[rate-filter-rules]-----
| none
-----
  
```

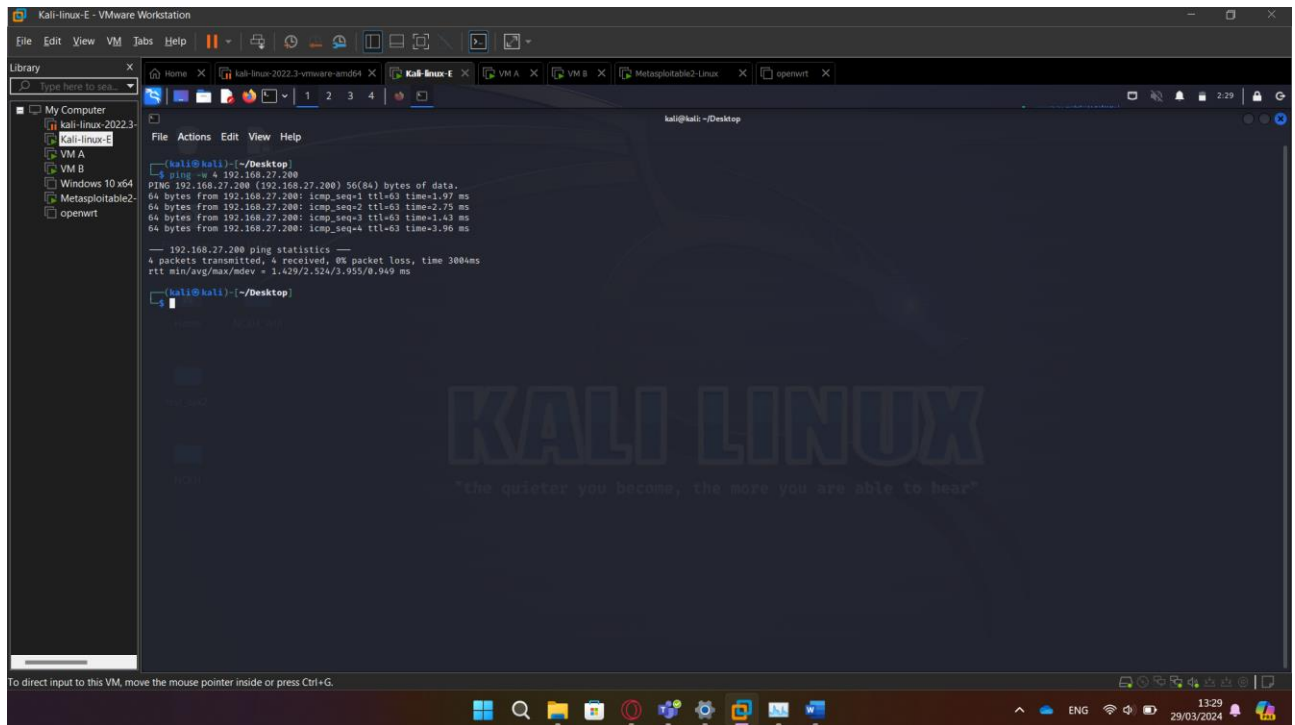
+ Máy router ping:

```

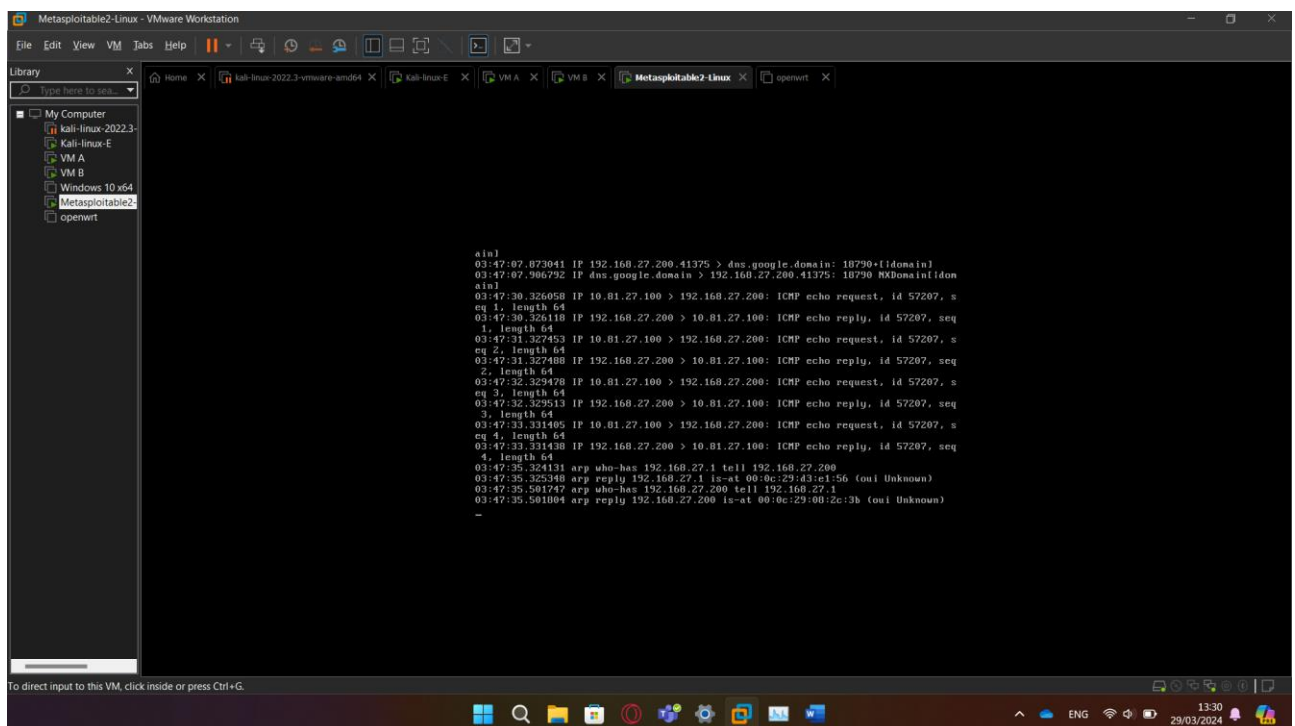
root@ubuntu2004:/
# Generated by iptables-save v1.8.4 on Mon Mar 25 05:00:09 2024
*filter
:INPUT ACCEPT [28:6834]
:FORWARD ACCEPT [8:672]
:OUTPUT ACCEPT [7:588]
-A FORWARD -i ens36 -o ens33 -m state --state RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -i ens36 -o ens38 -m state --state RELATED,ESTABLISHED -j ACCEPT
COMMIT
# Completed on Mon Mar 25 05:00:09 2024
root@ubuntu2004:/# ping 192.168.27.200
PING 192.168.27.200 (192.168.27.200) 56(84) bytes of data:
64 bytes from 192.168.27.200: icmp_seq=1 ttl=64 time=13.3 ms
64 bytes from 192.168.27.200: icmp_seq=2 ttl=64 time=37.1 ms
64 bytes from 192.168.27.200: icmp_seq=3 ttl=64 time=7.81 ms
^C
--- 192.168.27.200 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/ndev = 7.812/19.399/37.077/12.699 ms
root@ubuntu2004:/# ping -w 4 192.168.27.200
PING 192.168.27.200 (192.168.27.200) 56(84) bytes of data:
64 bytes from 192.168.27.200: icmp_seq=1 ttl=64 time=2.94 ms
64 bytes from 192.168.27.200: icmp_seq=2 ttl=64 time=2.81 ms
64 bytes from 192.168.27.200: icmp_seq=3 ttl=64 time=2.57 ms
64 bytes from 192.168.27.200: icmp_seq=4 ttl=64 time=2.29 ms
--- 192.168.27.200 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3023ms
rtt min/avg/max/ndev = 2.293/3.904/7.574/2.132 ms
root@ubuntu2004:/#
  
```

+ Kiểm tra log:

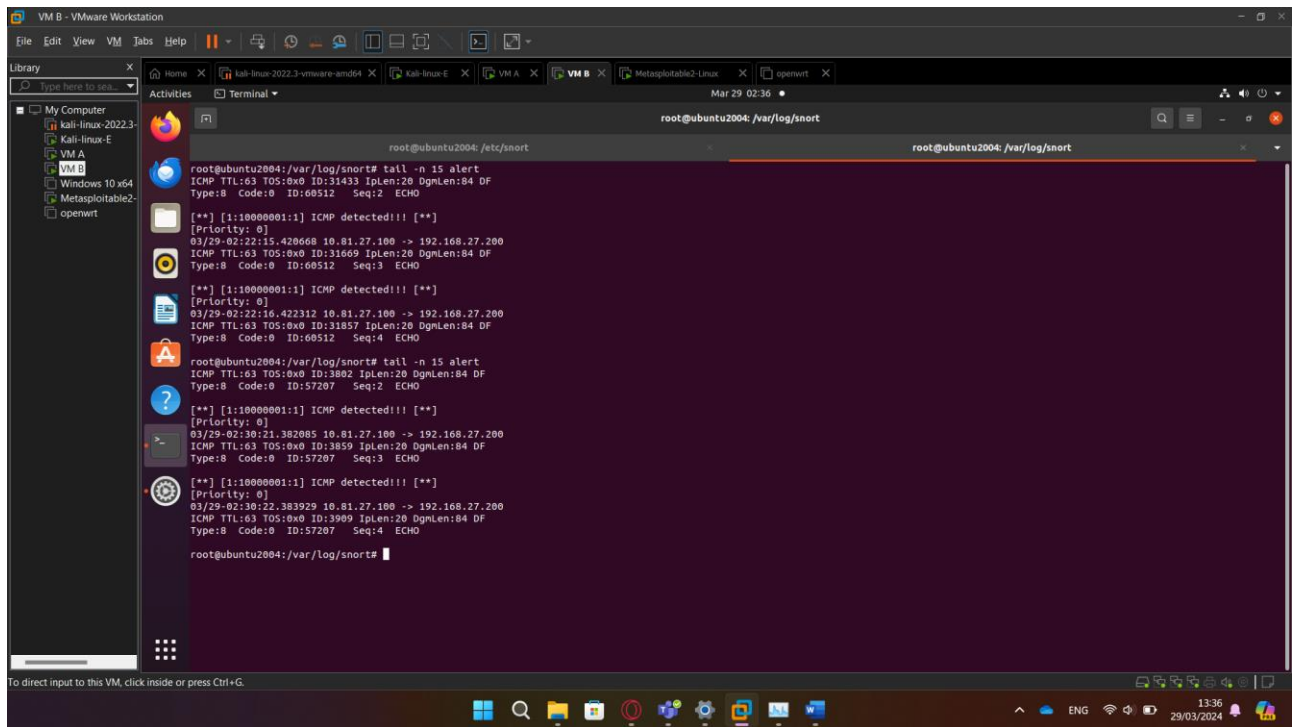




+ Tcpdump trên máy victim:

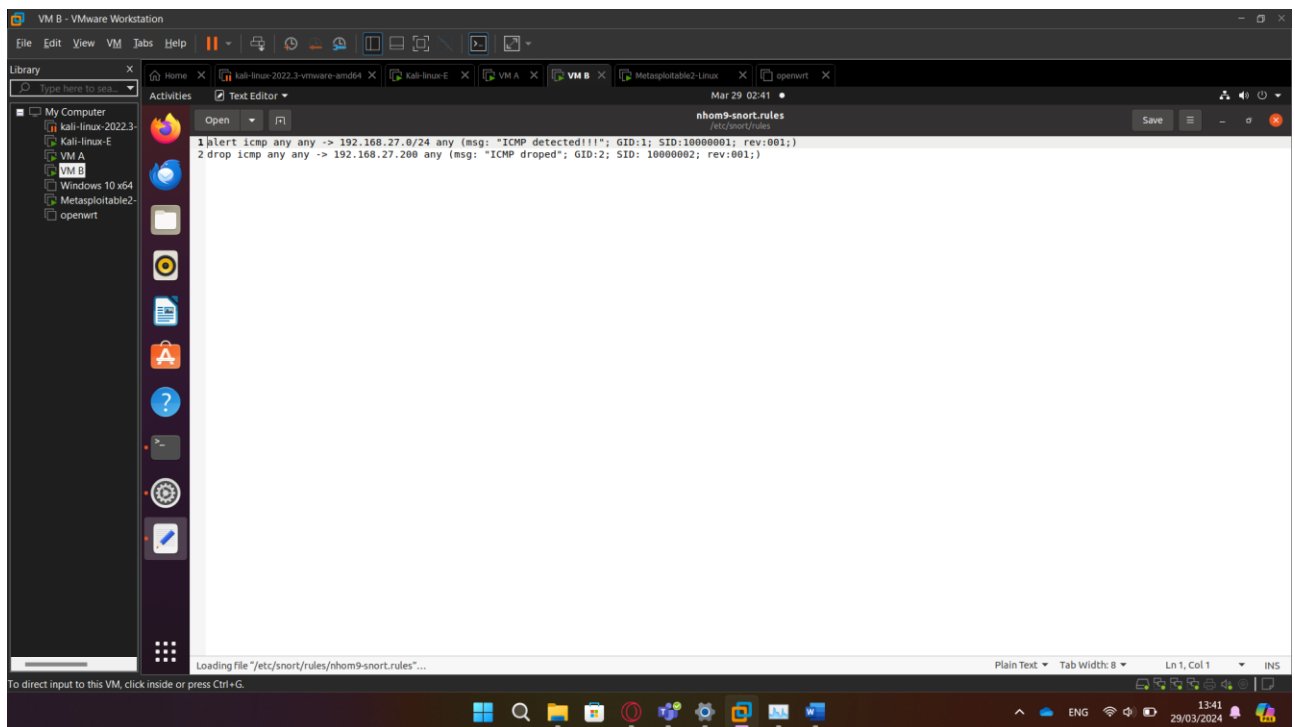


+ Alert log của snort:

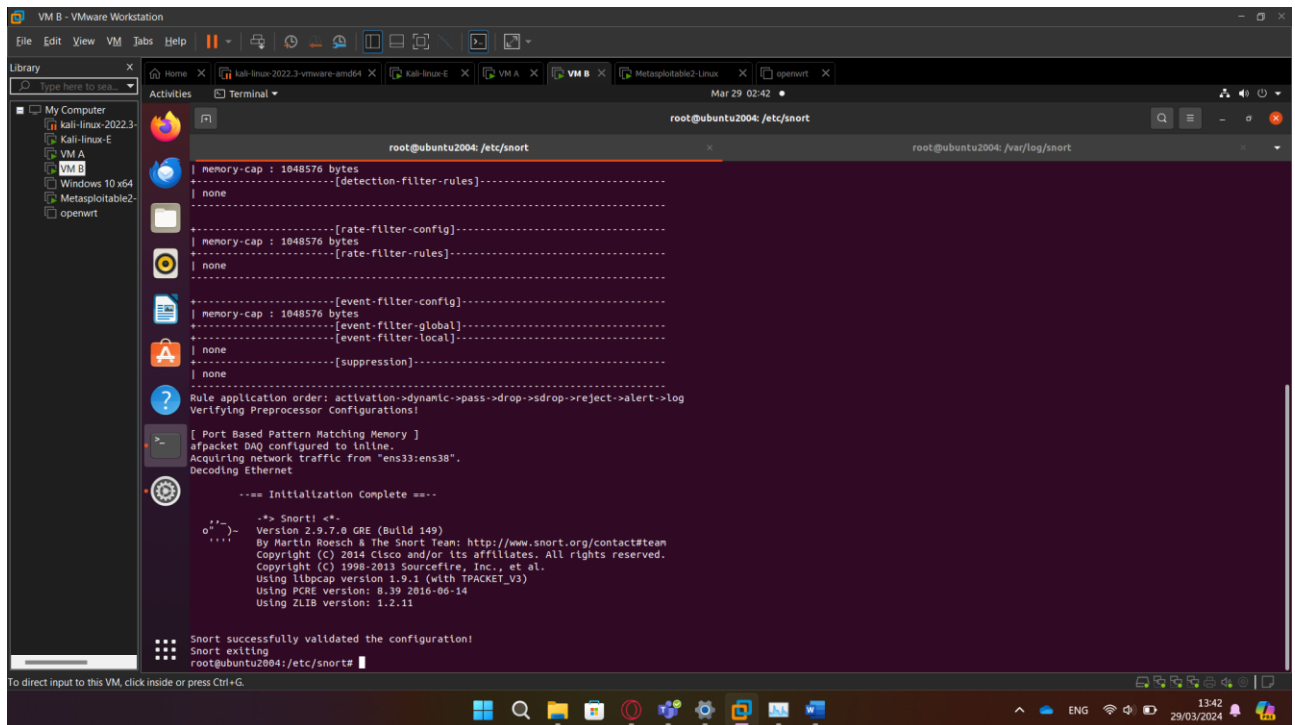


- Sau khi áp dụng rule #1.

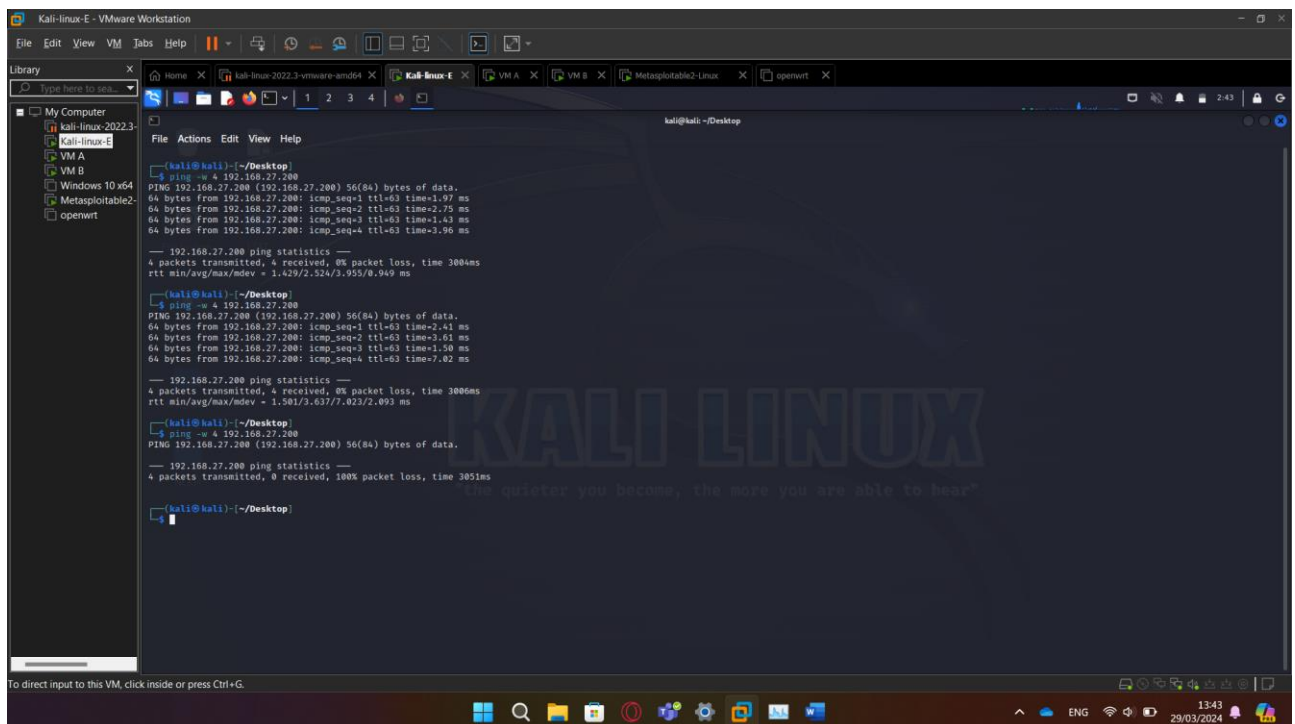
+ Thêm rule mới vào file rules:



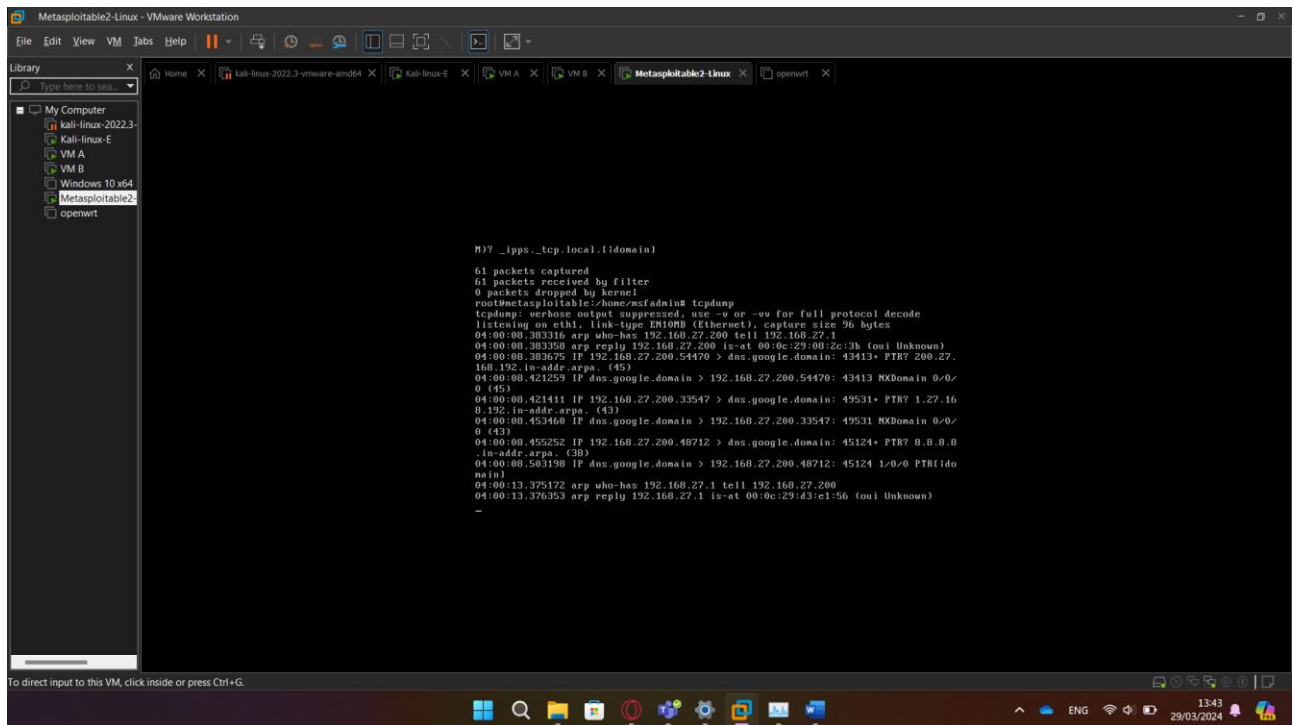
+ Kiểm tra rule:



+ Máy attacker ping đến victim:



+ Tcpdump ở máy Victim:



+ Alert log của snort, lúc này snort sẽ có 2 file alert: 1 file chứa thông báo drop (file alert), file còn lại chứa thông báo của alert (file alert.1):

